

Is there an algorithm that decides the solvability of a Diophantine equation with a finite number of solutions?

Apoloniusz Tyszk

Abstract

For a positive integer n , let $\theta(n)$ denote the smallest positive integer b such that for each system $S \subseteq \{x_i \cdot x_j = x_k, x_i + 1 = x_k : i, j, k \in \{1, \dots, n\}\}$ which has a solution in positive integers x_1, \dots, x_n and which has only finitely many solutions in positive integers x_1, \dots, x_n , there exists a solution of S in $([1, b] \cap \mathbb{N})^n$. We conjecture that there exists an integer $\delta \geq 9$ such that the inequality $\theta(n) \leq \left(2^{2^{n-5}} - 1\right)^{2^{n-5}} + 1$ holds for every integer $n \geq \delta$. We prove: (1) for every integer $n > 9$, the inequality $\theta(n) < \left(2^{2^{n-5}} - 1\right)^{2^{n-5}} + 1$ implies that $2^{2^{n-5}} + 1$ is composite, (2) the conjecture implies that there exists an algorithm which takes as input a Diophantine equation $D(x_1, \dots, x_p) = 0$ and returns the message "Yes" or "No" which correctly determines the solvability of the equation $D(x_1, \dots, x_p) = 0$ in positive integers, if the solution set is finite, (3) if a function $f: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ has a finite-fold Diophantine representation, then there exists a positive integer m such that $f(n) < \theta(n)$ for every integer $n > m$.

Key words and phrases: algorithmic decidability, Diophantine equation with a finite number of solutions, Fermat prime, finite-fold Diophantine representation, smallest solution of a Diophantine equation.

2010 Mathematics Subject Classification: 11U05.

In this article, we propose a conjecture which implies that there exists an algorithm which takes as input a Diophantine equation $D(x_1, \dots, x_p) = 0$ and returns the message "Yes" or "No" which correctly determines the solvability of the equation $D(x_1, \dots, x_p) = 0$ in positive integers, if the solution set is finite. Let

$$E_n = \{x_i \cdot x_j = x_k, x_i + 1 = x_k : i, j, k \in \{1, \dots, n\}\}$$

For a positive integer n , let $\theta(n)$ denote the smallest positive integer b such that for each system $S \subseteq E_n$ which has a solution in positive integers x_1, \dots, x_n and which has only finitely many solutions in positive integers x_1, \dots, x_n , there exists a solution of S in $([1, b] \cap \mathbb{N})^n$. We do not know whether or not there exists a computable function $\xi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ which is greater than the function $\theta: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$.

Theorem 1. *We have: $\theta(1) = 1$ and $\theta(2) = 2$. The inequality $\theta(n) \geq 2^{2^{n-2}}$ holds for every integer $n \geq 3$.*

Proof. Only $x_1 = 1$ solves the equation $x_1 \cdot x_1 = x_1$ in positive integers. Only $x_1 = 1$ and $x_2 = 2$ solve the system $\{x_1 \cdot x_1 = x_1, x_1 + 1 = x_2\}$ in positive integers. For each integer $n \geq 3$, the following system

$$\begin{cases} x_1 \cdot x_1 = x_1 \\ x_1 + 1 = x_2 \\ \forall i \in \{2, \dots, n-1\} x_i \cdot x_i = x_{i+1} \end{cases}$$

has a unique solution in positive integers, namely $(1, 2, 4, 16, 256, \dots, 2^{2^{n-3}}, 2^{2^{n-2}})$. \square

Theorem 2. For every positive integer n , $\theta(n+1) \geq \theta(n) \cdot \theta(n)$.

Proof. For every $k \in \{1, \dots, n\}$, if a system $S \subseteq E_n$ has only finitely many solutions in positive integers x_1, \dots, x_n , then the system $S \cup \{x_k \cdot x_k = x_{n+1}\}$ has only finitely many solutions in positive integers x_1, \dots, x_{n+1} . \square

Corollary 1. $\theta(1) = 1 < 2 = \theta(2) < \theta(3) < \theta(4) < \dots$

Primes of the form $2^{2^n} + 1$ are called Fermat primes, as Fermat conjectured that every integer of the form $2^{2^n} + 1$ is prime ([2, p. 1]). Fermat correctly remarked that $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, and $2^{2^4} + 1 = 65537$ are all prime ([2, p. 1]).

Open Problem. Are there infinitely many composite numbers of the form $2^{2^n} + 1$? ([2, p. 159])

Most mathematicians believe that $2^{2^n} + 1$ is composite for every integer $n \geq 5$.

Theorem 3. If $n \in \mathbb{N} \setminus \{0\}$ and $2^{2^n} + 1$ is prime, then the following system

$$\begin{cases} \forall i \in \{1, \dots, n\} x_i \cdot x_i = x_{i+1} \\ x_1 + 1 = x_{n+2} \\ x_{n+2} + 1 = x_{n+3} \\ x_{n+3} + 1 = x_{n+4} \\ x_{n+3} \cdot x_{n+5} = x_{n+4} \end{cases}$$

has a unique solution (a_1, \dots, a_{n+5}) in non-negative integers. The numbers a_1, \dots, a_{n+5} are positive and $\max(a_1, \dots, a_{n+5}) = a_{n+4} = (2^{2^n} - 1)^{2^n} + 1$.

Proof. The system equivalently expresses that $x_1^{2^n} + 1 = (x_1 + 2) \cdot x_{n+5}$. Therefore,

$$\begin{aligned} x_1^{2^n} + 1 &= ((x_1 + 2) - 2)^{2^n} + 1 = \\ &= 2^{2^n} + 1 + (x_1 + 2) \cdot \sum_{k=1}^{2^n} \binom{2^n}{k} \cdot (x_1 + 2)^{k-1} \cdot (-2)^{2^n-k} = (x_1 + 2) \cdot x_{n+5} \end{aligned}$$

Hence,

$$2^{2^n} + 1 = (x_1 + 2) \cdot \left(x_{n+5} - \sum_{k=1}^{2^n} \binom{2^n}{k} \cdot (x_1 + 2)^{k-1} \cdot (-2)^{2^n-k} \right)$$

Therefore, $x_1 + 2$ divides $2^{2^n} + 1$. Since $x_1 + 2 \geq 2$ and $2^{2^n} + 1$ is prime, we get $x_1 = 2^{2^n} - 1$.

Hence, $x_{n+2} = 2^{2^n}$ and $x_{n+3} = 2^{2^n} + 1$. Next, $x_{n+1} = x_1^{2^n} = (2^{2^n} - 1)^{2^n}$ and

$$x_{n+4} = x_{n+3} + 1 = (2^{2^n} - 1)^{2^n} + 1$$

The following positive integers

$$\begin{aligned}
\forall i \in \{1, \dots, n+1\} \ a_i &= (2^{2^n} - 1)^{2^{i-1}} \\
a_{n+2} &= 2^{2^n} \\
a_{n+3} &= 2^{2^n} + 1 \\
a_{n+4} &= (2^{2^n} - 1)^{2^n} + 1 \\
a_{n+5} &= 1 + \sum_{k=1}^{2^n} \binom{2^n}{k} \cdot (2^{2^n} + 1)^{k-1} \cdot (-2)^{2^n-k}
\end{aligned}$$

give the solution which is unique in non-negative integers. The number a_{n+5} is positive because

$$a_{n+5} = \frac{a_{n+4}}{a_{n+3}} = \frac{(2^{2^n} - 1)^{2^n} + 1}{2^{2^n} + 1}$$

□

Corollary 2. *For every integer $n > 5$, if $2^{2^{n-5}} + 1$ is prime, then*

$$\theta(n) \geq (2^{2^{n-5}} - 1)^{2^{n-5}} + 1$$

In particular,

$$\theta(9) \geq (2^{2^{9-5}} - 1)^{2^{9-5}} + 1 = (2^{16} - 1)^{16} + 1 > (2^{16} - 2^{15})^{16} = (2^{15})^{16} = 2^{240} > 2^{2^{9-2}}$$

The numbers $2^{2^{n-5}} + 1$ are prime when $n \in \{6, 7, 8\}$, but

$$\begin{aligned}
(2^{2^{6-5}} - 1)^{2^{6-5}} + 1 &= 10 < 65536 = 2^{2^{6-2}} \\
(2^{2^{7-5}} - 1)^{2^{7-5}} + 1 &= 50626 < 4294967296 = 2^{2^{7-2}} \\
(2^{2^{8-5}} - 1)^{2^{8-5}} + 1 &= 17878103347812890626 < 18446744073709551616 = 2^{2^{8-2}}
\end{aligned}$$

Corollary 3. *For every integer $n > 9$, the inequality $\theta(n) < (2^{2^{n-5}} - 1)^{2^{n-5}} + 1$ implies that $2^{2^{n-5}} + 1$ is composite.*

Conjecture. (cf. [7, p. 710]) *There exists an integer $\delta \geq 9$ such that the inequality*

$$\theta(n) \leq (2^{2^{n-5}} - 1)^{2^{n-5}} + 1$$

holds for every integer $n \geq \delta$.

Corollary 4. *By Corollary 1, the Conjecture implies that there exists a computable function $\xi: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ which is greater than the function $\theta: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$.*

Let α, β , and γ denote variables.

Lemma 1. ([6, p. 100]) For each positive integers x, y, z , $x + y = z$ if and only if

$$(zx + 1)(zy + 1) = z^2(xy + 1) + 1$$

Corollary 5. We can express the equation $x + y = z$ as an equivalent system \mathcal{F} , where \mathcal{F} involves x, y, z and 9 new variables, and where \mathcal{F} consists of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$.

Proof. The new 9 variables express the following polynomials:

$$zx, \quad zx + 1, \quad zy, \quad zy + 1, \quad z^2, \quad xy, \quad xy + 1, \quad z^2(xy + 1), \quad z^2(xy + 1) + 1$$

□

Lemma 2. Let $D(x_1, \dots, x_p) \in \mathbb{Z}[x_1, \dots, x_p]$. Assume that $\deg(D, x_i) \geq 1$ for each $i \in \{1, \dots, p\}$. We can compute a positive integer $n > p$ and a system $\mathcal{T} \subseteq E_n$ which satisfies the following two conditions:

Condition 1. For every positive integers $\tilde{x}_1, \dots, \tilde{x}_p$,

$$D(\tilde{x}_1, \dots, \tilde{x}_p) = 0 \iff \exists \tilde{x}_{p+1}, \dots, \tilde{x}_n \in \mathbb{N} \setminus \{0\} \text{ } (\tilde{x}_1, \dots, \tilde{x}_p, \tilde{x}_{p+1}, \dots, \tilde{x}_n) \text{ solves } \mathcal{T}$$

Condition 2. If positive integers $\tilde{x}_1, \dots, \tilde{x}_p$ satisfy $D(\tilde{x}_1, \dots, \tilde{x}_p) = 0$, then there exists a unique tuple $(\tilde{x}_{p+1}, \dots, \tilde{x}_n) \in (\mathbb{N} \setminus \{0\})^{n-p}$ such that the tuple $(\tilde{x}_1, \dots, \tilde{x}_p, \tilde{x}_{p+1}, \dots, \tilde{x}_n)$ solves \mathcal{T} .

Conditions 1 and 2 imply that the equation $D(x_1, \dots, x_p) = 0$ and the system \mathcal{T} have the same number of solutions in positive integers.

Proof. We write down the polynomial $D(x_1, \dots, x_p)$ and replace each coefficient by the successor of its absolute value. Let $\tilde{D}(x_1, \dots, x_p)$ denote the obtained polynomial. The polynomials $D(x_1, \dots, x_p) + \tilde{D}(x_1, \dots, x_p)$ and $\tilde{D}(x_1, \dots, x_p)$ have positive integer coefficients. The equation $D(x_1, \dots, x_p) = 0$ is equivalent to

$$D(x_1, \dots, x_p) + \tilde{D}(x_1, \dots, x_p) + 1 = \tilde{D}(x_1, \dots, x_p) + 1$$

There exist positive integers a and b and finite non-empty lists A and B such that the above equation is equivalent to

$$\begin{aligned} & \left(\left(\sum_{(i_1, j_1, \dots, i_k, j_k) \in A} x_{i_1}^{j_1} \cdot \dots \cdot x_{i_k}^{j_k} \right) + 1 \right) + \dots + 1 = \\ & \left(\left(\sum_{(i_1, j_1, \dots, i_k, j_k) \in B} x_{i_1}^{j_1} \cdot \dots \cdot x_{i_k}^{j_k} \right) + 1 \right) + \dots + 1 \end{aligned}$$

$a \text{ units}$ $b \text{ units}$

and all the numbers $k, i_1, j_1, \dots, i_k, j_k$ belong to $\mathbb{N} \setminus \{0\}$. Next, we apply Corollary 5. □

Theorem 4. The Conjecture implies that there exists an algorithm which takes as input a Diophantine equation $D(x_1, \dots, x_p) = 0$ and returns the message "Yes" or "No" which correctly determines the solvability of the equation $D(x_1, \dots, x_p) = 0$ in positive integers, if the solution set is finite.

Proof. We apply Lemma 2 and compute the system $\mathcal{T} \subseteq E_n$, where $n > p$. Let $w = \max(n, \delta)$. By Corollary 1, it suffices to check whether or not the system \mathcal{T} has a solution in positive integers x_1, \dots, x_n not greater than $\left(2^{2^{w-5}} - 1\right)^{2^{w-5}} + 1$. \square

The Davis-Putnam-Robinson-Matiyasevich theorem states that every recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a Diophantine representation, that is

$$(a_1, \dots, a_n) \in \mathcal{M} \iff \exists x_1, \dots, x_m \in \mathbb{N} \ W(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \quad (\text{R})$$

for some polynomial W with integer coefficients, see [3]. The polynomial W can be computed, if we know the Turing machine M such that, for all $(a_1, \dots, a_n) \in \mathbb{N}^n$, M halts on (a_1, \dots, a_n) if and only if $(a_1, \dots, a_n) \in \mathcal{M}$, see [3]. The representation (R) is said to be single-fold, if for every $a_1, \dots, a_n \in \mathbb{N}$ the equation $W(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ has at most one solution $(x_1, \dots, x_m) \in \mathbb{N}^m$. The representation (R) is said to be finite-fold, if for every $a_1, \dots, a_n \in \mathbb{N}$ the equation $W(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ has only finitely many solutions $(x_1, \dots, x_m) \in \mathbb{N}^m$. Yu. Matiyasevich conjectured that each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a single-fold (finite-fold) Diophantine representation, see [1, pp. 341–342] and [4, p. 42]. Currently, he seems agnostic on his conjectures, see [5, p. 749]. In [8, p. 581], the author explains why Matiyasevich's conjectures although widely known are less widely accepted.

Theorem 5. *If a function $f: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ has a finite-fold Diophantine representation, then there exists a positive integer m such that $f(n) < \theta(n)$ for every integer $n > m$.*

Proof. There exists a polynomial $W(x_1, x_2, x_3, \dots, x_r)$ with integer coefficients such that for each positive integers x_1, x_2 ,

$$(x_1, x_2) \in f \iff \exists x_3, \dots, x_r \in \mathbb{N} \setminus \{0\} \ W(x_1, x_2, x_3 - 1, \dots, x_r - 1) = 0$$

and for each positive integers x_1, x_2 at most finitely many tuples (x_3, \dots, x_r) of positive integers satisfy $W(x_1, x_2, x_3 - 1, \dots, x_r - 1) = 0$. By Lemma 2, there exists an integer $s \geq 3$ such that for every positive integers x_1, x_2 ,

$$(x_1, x_2) \in f \iff \exists x_3, \dots, x_s \in \mathbb{N} \setminus \{0\} \ \Phi(x_1, x_2, x_3, \dots, x_s) \quad (\text{E})$$

where $\Phi(x_1, x_2, x_3, \dots, x_s)$ is a conjunction of formulae of the forms $x_i + 1 = x_k$ and $x_i \cdot x_j = x_k$, the indices i, j, k belong to $\{1, \dots, s\}$, and for each positive integers x_1, x_2 at most finitely many tuples (x_3, \dots, x_s) of positive integers satisfy $\Phi(x_1, x_2, x_3, \dots, x_s)$. Let $[\cdot]$ denote the integer part function, and let an integer n be greater than $m = 2s + 2$. Then,

$$n \geq \left\lfloor \frac{n}{2} \right\rfloor + \frac{n}{2} > \left\lfloor \frac{n}{2} \right\rfloor + s + 1$$

and $n - \left\lfloor \frac{n}{2} \right\rfloor - s - 2 \geq 0$. Let T_n denote the following system with n variables:

$$\left\{ \begin{array}{l} \text{all equations occurring in } \Phi(x_1, x_2, x_3, \dots, x_s) \\ \forall i \in \left\{1, \dots, n - \left\lfloor \frac{n}{2} \right\rfloor - s - 2\right\} \ u_i \cdot u_i = u_i \\ \qquad \qquad \qquad t_1 \cdot t_1 = t_1 \\ \forall i \in \left\{1, \dots, \left\lfloor \frac{n}{2} \right\rfloor - 1\right\} \ t_i + 1 = t_{i+1} \\ \qquad \qquad \qquad t_2 \cdot t_{\left\lfloor \frac{n}{2} \right\rfloor} = u \\ \qquad \qquad \qquad u + 1 = x_1 \text{ (if } n \text{ is odd)} \\ \qquad \qquad \qquad t_1 \cdot u = x_1 \text{ (if } n \text{ is even)} \\ \qquad \qquad \qquad x_2 + 1 = y \end{array} \right.$$

By the equivalence (E), the system T_n is solvable in positive integers, $2 \cdot \left\lfloor \frac{n}{2} \right\rfloor = u$, $n = x_1$, and

$$f(n) = f(x_1) = x_2 < x_2 + 1 = y$$

The system T_n consists of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. Since T_n has only finitely many solutions in positive integers, $y \leq \theta(n)$. Hence, $f(n) < \theta(n)$. \square

Corollary 6. *The Conjecture contradicts Matiyasevich's conjecture on finite-fold Diophantine representations.*

References

- [1] M. Davis, Yu. Matiyasevich, J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*; in: Mathematical developments arising from Hilbert problems (ed. F. E. Browder), Proc. Sympos. Pure Math., vol. 28, Part 2, Amer. Math. Soc., Providence, RI, 1976, 323–378, <http://dx.doi.org/10.1090/pspum/028.2>; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., Providence, RI, 1996, 269–324.
- [2] M. Křížek, F. Luca, L. Somer, *17 lectures on Fermat numbers: from number theory to geometry*, Springer, New York, 2001.
- [3] Yu. Matiyasevich, *Hilbert's tenth problem*, MIT Press, Cambridge, MA, 1993.
- [4] Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done*; in: Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 1–47, Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000, <http://dx.doi.org/10.1090/conm/270>.
- [5] Yu. Matiyasevich, *Towards finite-fold Diophantine representations*, J. Math. Sci. (N. Y.) vol. 171, no. 6, 2010, 745–752, <http://dx.doi.org/10.1007%2Fs10958-010-0179-4>.
- [6] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic 14 (1949), no. 2, 98–114, <http://dx.doi.org/10.2307/2266510>; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., Providence, RI, 1996, 7–23.
- [7] A. Tyszka, *A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions*, Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (eds. M. Ganzha, L. Maciaszek, M. Paprzycki); *Annals of Computer Science and Information Systems*, vol. 5, 709–716, IEEE Computer Society Press, 2015, <http://dx.doi.org/10.15439/2015F41>.
- [8] A. Tyszka, *All functions $g: \mathbb{N} \rightarrow \mathbb{N}$ which have a single-fold Diophantine representation are dominated by a limit-computable function $f: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$ which is implemented in MuPAD and whose computability is an open problem*; in: Computation, cryptography, and network security (eds. N. J. Daras and M. Th. Rassias), Springer, Cham, Switzerland, 2015, 577–590, http://dx.doi.org/10.1007/978-3-319-18275-9_24.

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 116B, 30-149 Kraków, Poland
E-mail: rttyszka@cyf-kr.edu.pl